ทฤษฎีจำนวน

คุณสมบัติบางประการของจำนวนเต็ม

การหารลงตัว (exact division)

บทนิยาม 1 การหารลงตัว

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า a หาร b ลงตัว ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ทำให้ $b = ac$ ใช้สัญลักษณ์ $a \mid b$ แทน a หาร b ลงตัว

ถ้า $a \mid b$ เราเรียก a ว่าตัวหาร (divisor) หรือตัวประกอบ (factor) ของ b และเรียก b ว่า พหุคูณ (multiple) ของ a และ ถ้า a หาร b ไม่ลงตัวเขียนแทนด้วย $a \nmid b$

ตัวอย่างที่ 1 จงพิจารณาว่า $6 \mid 1098$, $15 \mid (-255)$, $4 \mid 522$ หรือไม่

วิธีทำ เนื่องจาก 1098 = 6( ) ดังนั้น $6 \mid 1098$

ข้อสังเกต สำหรับจำนวนเต็ม a ใด ๆ จะได้ว่า

1. ถ้า $a \neq 0$ แล้ว $a \mid 0$ และ $a \mid a$
2. $a \mid 1$ ก็ต่อเมื่อ $a = 1$ หรือ $a = -1$

ตัวอย่างที่ 2 จงหาตัวหารทั้งหมดของ 100

ตัวหารทั้งหมดของ 100 คือ

ทฤษฎีบท 1 ให้ a, b และ c เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ จะได้ว่า

1. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
2. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = \pm b$
3. ถ้า $a \mid b$ แล้ว $a \mid bc$ สำหรับทุก ๆ จำนวนเต็ม c
4. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$
5. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx+cy)$ เมื่อ x และ y เป็นจำนวนเต็มใด ๆ
6. ถ้า $a \mid (b+c)$ และ $a \mid b$ แล้ว $a \mid c$

ตัวอย่างที่ 3 พิจารณาสมบัติของการหารลงตัว

1) เนื่องจาก -3 | 42 และ 42 | 378 ดังนั้นจะได้
2) เนื่องจาก 11 | (33+143) และ 11 | 33 ดังนั้นจะได้

บทนิยาม 2 ให้ x เป็นจำนวนจริงใดๆ จำนวนเต็มที่มากที่สุดซึ่งน้อยกว่าหรือเท่ากับ x จะเขียนแทนด้วย $\lceil x \rceil$

เช่น $\lceil 51.2 \rceil = 51$, $\lceil -1.2 \rceil = -2$, $\left\lceil \frac{100}{8} \right\rceil = 12$

ตัวอย่างที่ 4

1) มีจำนวนเต็มตั้งแต่ 1 ถึง 200 กี่จำนวนที่ 4 หารลงตัว

2) มีจำนวนเต็มตั้งแต่ 100 ถึง 500 กี่จำนวนที่ 9 หารลงตัว

จำนวนเฉพาะ (prime number)

บทนิยาม 3 จำนวนเต็มบวก p ที่มากกว่า 1 เป็น**จำนวนเฉพาะ** (prime) ก็ต่อเมื่อตัวประกอบที่เป็นบวกของ p คือ 1 และ p เท่านั้น และเรียกจำนวนเต็มบวกที่มากกว่า 1 ที่ไม่เป็นจำนวนเฉพาะว่า **จำนวนประกอบ** (composite)

เช่น 11 เป็นจำนวนเฉพาะ เพราะมีตัวประกอบที่เป็นบวก คือ 1 และ 11 เท่านั้น

15 เป็นจำนวนประกอบ เพราะมีตัวประกอบที่เป็นบวก คือ 3 และ 5

ทฤษฎีบท 2 ทฤษฎีบทหลักมูลของเลขคณิต (The fundamental theorem of arithmetic)

ทุก ๆ จำนวนเต็มบวก n ที่มากกว่า 1 จะได้ว่า n เป็นจำนวนเฉพาะหรือ n สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น โดยไม่รวมการสลับที่ตัวคูณหรือการคูณด้วย 1

ข้อสังเกต ทุกจำนวนเต็มบวก n ที่มากกว่า 1 จะได้ว่า n เป็นจำนวนเฉพาะ หรือ n สามารถแยกตัวประกอบที่เป็นจำนวนเฉพาะได้เพียงรูปเดียวเท่านั้น คือ

$n = p_1^{c_1} p_2^{c_2} p_3^{c_3} \cdots p_k^{c_k}$ โดยที่ $p_1 < p_2 < p_3 < \cdots < p_k$ เป็นจำนวนเฉพาะ C_i เป็นจำนวนเต็มบวก ทุก $i = 1, 2, 3, \ldots, k$ และ เรียก n ที่เขียนในรูปแบบข้างต้นว่า รูปแบบบัญญัติ

ตัวอย่างที่ 5 จงเขียนรูปแบบบัญญัติของ 300, 101, 693 และ 2048

$300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5$

$101 =$

$693 =$

$2048 =$

ทฤษฎีบท 3 ถ้า n เป็นจำนวนประกอบที่มากกว่า 1 แล้ว n จะมีตัวหารที่เป็นจำนวนเฉพาะ p โดยที่ p จะน้อยกว่า หรือเท่ากับ $\sqrt{n}$

จาก **ทฤษฎีบท** *3* จะได้ว่า

“ถ้า n ไม่มีตัวหารที่เป็นจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ แล้วจะได้ว่า n เป็นจำนวนเฉพาะ”

ตัวอย่างที่ 6 จงแสดงว่า 101 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{101}$ คือ 2, 3, 5 และ 7

เนื่องจาก 2, 3, 5 และ 7 หาร 101 ไม่ลงตัวดังนั้น 101 เป็นจำนวนเฉพาะ

ตัวอย่างที่ 7 จงแสดงว่า 2873 เป็นจำนวนเฉพาะหรือไม่

ตัวอย่างที่ 8 จงหาจำนวนเฉพาะที่มีค่ามากที่สุดที่เป็นตัวประกอบของ 1365

ตัวอย่างที่ 9 จงหาจำนวนตัวหารทั้งหมดของ 4725

ทฤษฎีบท 4 จำนวนเฉพาะมีอยู่เป็นจำนวนอนันต์

ขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n

1. หา $\sqrt{n}$
2. หาจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$
3. พิจารณาว่าจำนวนเฉพาะ p ในขั้นที่ 2. จำนวนใดที่เป็นตัวประกอบของ n บ้าง โดยเริ่มจากจำนวนเฉพาะที่มีค่าน้อยที่สุดก่อน
   3.1. ถ้าไม่มีจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ จำนวนใดเลยที่หาร n ลงตัว จะได้ว่า n เป็นจำนวนเฉพาะ และจบขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n
   3.2. ถ้ามีจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ และหาร n ลงตัว แล้วจะได้ว่า n จะเป็นจำนวนประกอบ ซึ่งในขั้นตอนนี้ จะได้ตัวประกอบที่เป็นจำนวนเฉพาะตัวหนึ่งของ n เท่านั้น
   สมมติให้เป็น p_1 ดังนั้นได้ $\frac{n}{p_1}$ เป็นจำนวนเต็มทำขั้นตอนที่ 4. ต่อ
4. ทำซ้ำขั้นที่ 1. , 2. และ 3. กับจำนวน $\frac{n}{p_1}$ซึ่งจะสังเกตเห็นว่า ถ้า $\frac{n}{p_1}$มีตัวประกอบที่เป็นจำนวนเฉพาะให้เป็น p_2 แล้วจะได้ว่า $p_1 \leq p_2$และ $\frac{n}{p_1 p_2}$ เป็นจำนวนเต็ม
5. ทำซ้ำขั้นที่ 1. , 2. และ 3. กับจำนวน $\frac{n}{p_1 p_2}$เช่นนี้เรื่อย ๆ
   ขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n นี้จะจบเมื่อ $\frac{n}{p_1 p_2 \cdots p_k}$เป็นจำนวนเฉพาะ

ตัวอย่างที่ 10 จงหาตัวประกอบที่เป็นจำนวนเฉพาะทั้งหมดของ 77077

แบบฝึกหัด

1. จงพิจารณาว่า 163, 10001 เป็นจำนวนเฉพาะหรือเป็นจำนวนประกอบ
2. จงแยกตัวประกอบของ 707
3. จงหาตัวประกอบที่เป็นจำนวนเฉพาะของจำนวนต่อไปนี้
   3.1. 987
   3.2. 2222
   3.3. 729
   3.4. 505050
4. จงเขียนโปรแกรมเพื่อหาตัวประกอบทุกตัวของจำนวนเต็มบวกที่ผู้ใช้ป้อนเข้า
5. จงเขียนโปรแกรมหาว่าจำนวนเต็มที่ผู้ใช้ป้อนเข้าเป็นจำนวนเฉพาะหรือจำนวนประกอบ
6. จงเขียนโปรแกรมเพื่อหาจำนวนเฉพาะตั้งแต่ 1 ถึง 100
7. ข้อความคาดเดาของคริสเตียนโกลบัค (Gold bach) กล่าว*ว่า*
   “สำหรับทุก ๆ จำนวนเต็มคู่ที่มากกว่า 4 จะเป็นผลบวกของจำนวนเฉพาะคี่สองจำนวน”
   (6＝3＋3, 8＝3＋5, 10＝5＋5, 12＝5＋7, 14＝7＋7, 16＝5＋11 เป็นต้น*)*
   จงเขียนโปรแกรมเพื่อหาผลบวกที่เป็นจำนวนเฉพาะคี่สองจำนวนของจำนวนเต็มคู่ตั้งแต่ 2 ถึง 40
8. จงเขียนโปรแกรมเพื่อหาตัวประกอบเฉพาะทั้งหมดของจำนวนเต็มที่ผู้ใช้ป้อนเข้า

ทฤษฎีบท 5 ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a และ b เป็นจำนวนเต็ม และ $b \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงชุดเดียวที่ทำให้ $a = bq + r$ เมื่อ $0 \leq r < |b|$

เรียก a ว่า ตัวตั้ง (dividend)

b ว่า ตัวหาร (divisor)

q ว่า ผลหาร (quotient) และ

r ว่า เศษเหลือ (remainder)

ตัวอย่างที่ 11 จงหาผลหารและเศษจากการหาร

1) 400 ด้วย 120

2) 5 ด้วย 7

3) 140 ด้วย -72

4) -175 ด้วย 50

5) -245 ด้วย -70

ตัวหารร่วมมากและตัวคูณร่วมน้อย

นิยาม 4 จำนวนเต็ม a จะเป็นจำนวนคู่ ก็ต่อเมื่อ สามารถเขียน $a = 2m$ เมื่อ m เป็นจำนวนเต็ม
จำนวนเต็ม a จะเป็นจำนวนคี่ ก็ต่อเมื่อ สามารถเขียน $a = 2n+1$ เมื่อ n เป็นจำนวนเต็ม
จำนวนเต็มที่หาร a และ b ลงตัว เราจะเรียกว่าตัวหารร่วมของ a และ b

ตัวอย่างที่ 12 จงหาเซตตัวหารร่วมทั้งหมดของ 36 และ 42

วิธีทำ ให้ A และ B แทนเซตของตัวหารทั้งหมดของ 36 และ 42 ตามลำดับ จะได้

$A = \{ -36, -18, -9, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 18, 36 \}$

$B = \{ -42, -21, -7, -6, -3, -2, -1, 1, 2, 3, 6, 7, 21, 42 \}$

เพราะฉะนั้น เซตของตัวหารร่วมทั้งหมดของ 36 และ 42 คือ

นิยาม 5 ตัวหารร่วมมาก (Greatest Common Divisor : GCD)

ให้ a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ จำนวนเต็มบวกที่มากที่สุด d ซึ่ง $d \mid a$ และ $d \mid b$ เรียก d ว่า ตัวหารร่วมมาก (ห.ร.ม.) ของ a และ b แทนด้วย (a, b)

ตัวอย่างที่ 13 จงหา (36, 48) และ (17, 22)

ข้อสังเกต

1) $(a, b) = (a, -b) = (-a, b) = (-a, -b) = (b, a)$
2) $(a, 0) = (0, a) = |a|$ เมื่อ $a \neq 0$
3) ถ้า $a \mid b$ แล้ว $(a, b) = |a|$
4) ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid (a, b)$

ตัวอย่างที่ 14 จากข้อสังเกตข้างต้นจะได้ว่า

1) (12, 20) =

2) (6, 15) =

3) (-7, 0) =

4) เนื่องจาก -8 | 16 ดังนั้น

5) เนื่องจาก 7 | 42 และ 7 | 56 ดังนั้น

นิยาม 6 ตัวคูณร่วมน้อย (Least Common Multiple: LCM)

ตัวคูณร่วมน้อย (ค.ร.น.) ของจำนวนเต็มบวก a และ b เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ a และ b หารลงตัว แทนด้วย [a, b]

ตัวอย่างที่ 15 จงหา [15, 20] และ [24, 36]

ทฤษฎีบท 6 ให้ a และ b เป็นจำนวนเต็มบวกแล้ว $ab = (a,b)\cdot[a,b]$

พิจารณา *[24, 36] =*

(24, 36) =

ขั้นตอนวิธีแบบยูคลิด (Euclidean algorithm)

ขั้นตอนวิธีหนึ่งที่สำคัญและเป็นขั้นตอนวิธีเก่าแก่ที่สุดในทางคณิตศาสตร์ คือ ขั้นตอนวิธีของยูคลิด เป็นขั้นตอนที่เราสามารถนำมาใช้หาตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวน หรือใช้ในการแก้ปัญหาที่ใช้ทฤษฎีบทเศษเหลือของจีน

พิจารณาขั้นตอนต่อไปนี้ *(เขียนในฟอร์ม $a = bq + r$)*

287 = 91(3) + 14 *($a = 287, b=91$ พบ $q=3$ และ $r=14$)*

91 = 14(6) + 7 *(ต่อมา a <- b และ b <- r คำนวณหา q และ r รอบใหม่)*

14 = 7(2)

จะได้ว่า (14, 7) = 7, (91, 7) = 7 และ (287, 7) = 7

ทฤษฎีบท 7 ให้ $a = bq + r$ เมื่อ a, b, q และ r เป็นจำนวนเต็ม แล้ว $(a, b) = (b, r)$

ขั้นตอนวิธีแบบยูคลิด

สำหรับจำนวนเต็มบวก a, b เมื่อ $a \geq b$ และ $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n$ เป็นจำนวนเต็ม โดยที่

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b \\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

แล้วจะได้ว่า $(a, b) = r_n$

ตัวอย่างที่ 16 จงหา (527, 3553) โดยใช้ขั้นตอนวิธีแบบยูคลิด

The Euclidean Algorithm

Input : a and b (non negative not both zero)

Output : Greatest common divisor of a and b

Procedure gcd (a, b : positive integers)

// make a largest

if $a < b$ then

swap (a , b)

while $b \neq 0$ do

begin

divide a by b to obtain $a = bq + r$, $0 \leq r < b$

$a = b$

$b = r$

end

return (a)

end // gcd (a, b) is a

ทฤษฎีบท 8 ให้ b เป็นจำนวนเต็มบวกที่มากกว่า 1 จะได้ว่าทุกจำนวนเต็มบวก a เขียนให้อยู่ในรูป

$$a = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_2 b^2 + a_1 b + a_0$$

ได้เพียงแบบเดียวเท่านั้น โดยที่ n เป็นจำนวนเต็มบวก และ a_i เป็นจำนวนเต็มซึ่ง $0 \leq a_i < b$ ทุกค่า $i = 0, 1, 2, \ldots, n$ และเรียกสมการดังกล่าวว่า **การเขียนจำนวนเต็ม a ในเลขฐาน b**

หมายเหตุ กรณีที่ $b = 10$ จะได้ว่า

กรณีที่ b = 2 จะได้ว่า

ตัวอย่างที่ 17 1) จงเปลี่ยน 101011011_2 เป็นเลขฐานสิบ

2) จงเปลี่ยน 123 เป็นเลขฐานสอง

นิยาม 7 จำนวนเต็ม a และ b ที่ไม่เป็นเป็นศูนย์พร้อมกัน เป็นจำนวนเฉพาะสัมพัทธ์ (relative prime number) ถ้า $(a, b) = 1$

ตัวอย่างที่ 18 1) เนื่องจาก (14, 45) = 1 ดังนั้น 14 และ 45 เป็นจำนวนเฉพาะสัมพัทธ์

2) เนื่องจาก (14, 41) = 1 ดังนั้น 14 และ 41 เป็นจำนวนเฉพาะสัมพัทธ์

นิยาม 8 ถ้า $(a_1, a_2, ..., a_n) = 1$ เราจะเรียก $a_1, a_2, ..., a_n$ ว่าเป็นจำนวนเฉพาะสัมพัทธ์ และถ้าทุก i, j ที่ $i \neq j$ และ $(a_i, a_j) = 1$ เราจะเรียก $a_1, a_2, ..., a_n$ ว่าเป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ (pair wise relatively prime numbers)

ตัวอย่างที่ 19 จงพิจารณาว่า 15, 17 และ 28 เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่หรือไม่

ทฤษฎีบท 9 สำหรับจำนวนเต็ม a , b ใด ๆ ถ้า $d = (a , b)$ แล้ว จะได้ว่า $\left(\frac{a}{d},\frac{c}{d}\right) = 1$

ทฤษฎีบท 10 ถ้า $(a, b) = (a, c) = 1$ จะได้ว่า $(a, bc) = 1$

ทฤษฎีบท 11 ถ้า a และ b เป็นจำนวนเต็มบวกจะมีจำนวนเต็ม x และ y ซึ่ง $(a, b) = ax + by$ เรียก $ax + b$ ว่าผลรวมเชิงเส้น (Linear Combination)

ตัวอย่างที่ 18 จงเขียน (252, 198) = 18 ในรูปผลรวมเชิงเส้นของ 252 และ 198

บทแทรก ถ้า a, b และ c เป็นจำนวนเต็มบวก ซึ่ง $(a, b) = 1$ และ $a \mid bc$ แล้ว $a \mid c$

สมการไดโอแฟนไทน์เชิงเส้น (Linear Diophantine Equation)

สมการไดโอแฟนไทน์เชิงเส้น คือ สมการเชิงเส้นที่มีตัวแปรมากกว่าหรือเท่ากับหนึ่งตัวแปร โดยที่ผลเฉลยของสมการเป็นจำนวนเต็ม

สมการไดโอแฟนไทน์เชิงเส้นแบบง่ายที่สุด คือ สมการไดโอแฟนไทน์เชิงเส้นสองตัวแปร ซึ่งมีรูปทั่วไปดังนี้

$ax + by = c$ เมื่อ $a, b, c \in I$ และ $a, b \neq 0$

การหาผลเฉลยของสมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร ก็คือการหาค่าของตัวแปร x, y ที่เป็นจำนวนเต็มที่ทำให้สมการเป็นจริง

เช่น กำหนดสมการไดโอแฟนไทน์เชิงเส้น $49x + 21y = 903$

ผลเฉลยของสมการที่เป็นไปได้ คือ (9, 11), (10, 14)

บางสมการอาจจะไม่มีผลเฉลย เช่น สมการ $2x + 6y = 33$

ทฤษฎีบท 12 ให้ a, b และ c เป็นจำนวนเต็ม $a \neq 0$ และ $b \neq 0$ โดยที่ $d = (a, b)$ จะได้ว่า

1. สมการ $ax + by = c$ ไม่มีผลเฉลย ถ้า $d \nmid c$
2. สมการ $ax + by = c$ ถ้า $d \mid c$ แล้ว สมการจะมีผลเฉลยหลายผลเฉลยนับไม่ถ้วน

และ ถ้าให้ x_0 และ y_0 เป็นผลเฉลยเฉพาะชุดแรกของสมการแล้ว ผลเฉลยทั้งหมดของสมการจะอยู่ในรูปทั่วไป คือ

$$x = x_0 + \left(\frac{b}{d}\right)n \text{ และ } \quad y = y_0 - \left(\frac{a}{d}\right)n \quad \text{เมื่อ } n \in I$$

ตัวอย่างที่ 21 จงพิจารณาว่าสมการต่อไปนี้ข้อใดบ้างที่มีผลเฉลยเป็นจำนวนเต็ม และถ้าข้อใดมี จงหาผลเฉลยที่เป็นจำนวนเต็มทั้งหมดด้วย

1) $4x + 2y = 11$

2) $2x + 6y = 8$

ตัวอย่างที่ 22 ชายคนหนึ่งต้องการซื้อตั๋วเดินทางเป็นจำนวน 510 บาท โดยเขาจะซื้อตั๋วเดินทางชนิดละ 20 บาท และชนิดละ 50 บาท จงหาว่า เขาสามารถซื้อตั๋วเดินทางแต่ละชนิดได้อย่างละเท่าไร

แบบฝึกหัด

1. จำนวนสมบูรณ์ (perfect number) คือจำนวนเต็มบวก ที่มีค่าเท่ากับผลบวกของตัวหารแท้ของมันเอง
   จงเขียนโปรแกรมเพื่อทำงานต่อไปนี้
   a. ตรวจสอบว่าจำนวนเต็มที่ผู้ใช้ป้อนเข้าเป็นจำนวนสมบูรณ์หรือไม่
   b. หาจำนวนสมบูรณ์ที่น้อยกว่า 10000 และ นับว่าตั้งแต่ 1 ถึง 10000 มีจำนวนสมบูรณ์อยู่ทั้งหมดกี่จำนวน
2. จงเขียนโปรแกรมเพื่อหาตัวหารร่วมมากของจำนวนสองจำนวนที่ผู้ใช้ป้อนเข้า
3. จงเขียนโปรแกรมเพื่อหาตัวคูณร่วมน้อยของจำนวนสองจำนวนที่ผู้ใช้ป้อนเข้า
4. จงเขียนโปรแกรมเพื่อหาตัวหารร่วมมากของจำนวนสามจำนวนที่ผู้ใช้ป้อนเข้า
5. จงเขียนโปรแกรมเพื่อหาเศษส่วนอย่างต่ำของจำนวนที่ผู้ใช้ป้อนเข้า
6. จงเขียนโปรแกรมเพื่อตรวจสอบว่าจำนวนเต็มที่ผู้ใช้ป้อนเข้า 3 จำนวนเป็นจำนวนเฉพาะสัมพัทธ์ ทุกคู่หรือไม่
7. จงเขียนโปรแกรมเพื่อแปลงเลขฐาน 10 เป็นฐาน 2 และจากเลขฐาน 2 เป็นฐาน 10

สมภาค (Congruence)

คาร์ล ฟรีดริค เกาส์ (Carl Friedrich Gauss) นักคณิตศาสตร์ชาวเยอรมันได้พัฒนาเกี่ยวกับแนวความคิดเรื่องสมภาคเมื่อปลายศตวรรษที่ *18* ได้สร้างทฤษฎีบทที่สำคัญ ๆ ทางทฤษฎีจำนวนขึ้นหลายทฤษฎี ซึ่งเป็นประโยชน์อย่างมากในการนำไปประยุกต์ใช้

นิยาม 9 กำหนดให้ a เป็นจำนวนเต็มและ m เป็นจำนวนเต็มบวก เศษเหลือจากการหาร a ด้วย m สามารถเขียนแทนด้วย $a \bmod m$

จากขั้นตอนวิธีการหาร a ด้วย m จะได้ $a = mq + r$ เมื่อ $0 \le r < |d|$ นั่นคือ $a \bmod m = r$

ตัวอย่างที่ 23 19 mod 5 =

136 mod 9 =

2013 mod 101 =

นิยาม 10 ถ้า a และ b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวกแล้ว a คอนกรูเอนซ์กับ b โมดูโล m (a congruent to b modulo m) ก็ต่อเมื่อ $m \mid (a - b)$ เขียนแทนด้วย $a \equiv b \pmod m$

ข้อสังเกต $a \equiv b \pmod m \leftrightarrow a \bmod m = b \bmod m$

ตัวอย่างที่ 24 $17 \equiv 5 \pmod 6$?

$27 \equiv 14 \pmod 6$?

ทฤษฎีบท 13 ให้ m เป็นจำวนเต็มบวก และ a, b, c และ d เป็นจำนวนเต็มใด ๆ จะได้ว่า

1. ถ้า $a \equiv b \pmod m$ แล้ว $b \equiv a \pmod m$
2. ถ้า $a \equiv b \pmod m$ และ m_1 เป็นจำนวนเต็มบวกที่ $m_1 \mid m$ แล้ว $a \equiv b \pmod{m_1}$
3. ถ้า $a \equiv b \pmod m$ แล้ว $ca \equiv cb \pmod{|c|m}$ เมื่อ $c \neq 0$
4. ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว $a + c \equiv b + d \pmod m$
5. ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว $ac \equiv bd \pmod m$
6. ถ้า $a \equiv b \pmod m$ แล้ว $a^n \equiv b^n \pmod m$ เมื่อ n เป็นจำนวนเต็มบวกใด ๆ

ตัวอย่างที่ 25 จงหาเศษที่ได้จากการหาร 7^{10} ด้วย 51

ทฤษฎีบท 14 ให้ m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็มใด ๆ จะได้ว่า

1. $a \equiv r \pmod{m}$ และ $0 \le r < m$ ก็ต่อเมื่อ r เป็นเศษเหลือจากการหาร a ด้วย m
2. ให้ $0 \le r, s < m$ จะได้ว่า $r \equiv s \pmod{m}$ ก็ต่อเมื่อ $r = s$
3. $a \equiv b \pmod{m}$ ก็ต่อเมื่อเศษเหลือจากการหาร a และ b ด้วย m เท่ากัน

ทฤษฎีบท 15 ให้ m เป็นจำนวนเต็มบวกและให้ a, b และ c เป็นจำนวนเต็ม
ถ้า $ac \equiv bd \pmod{m}$ และ $\gcd(c, m) = 1$ แล้ว $a \equiv b \pmod{m}$

แบบฝึกหัด

1. จงหาหลักหน่วยของ 6^{50}, 11^{99}
2. จงหาเลขสองหลักสุดท้ายของ 11^{99}, 11^{300}
3. จงหาเศษเหลือจากการหาร $23^3 \times 49$ ด้วย 25
4. จงหาเศษเหลือจากการหาร $3^{100} \times 5$ ด้วย 13

การประยุกต์ของสมภาค

เลขมาตรฐานสากลประจำหนังสือ (International Standard Book Numbers :ISBN)

ISBN เป็นรหัสที่ใช้จำแนกหนังสือ ประกอบด้วยรหัส 10 อักขระ เช่น 974-472-362-9 แบ่งเป็น 4 ส่วน คือ

ส่วนที่ 1 มีอักขระ 3 ตัว เป็นรหัสประเทศ

ส่วนที่ 2 มีอักขระ 3 ตัว เป็นรหัส โรงพิมพ์

ส่วนที่ 3 มีอักขระ 3 ตัว เป็นรหัส จำแนกหนังสือในโรงพิมพ์

ส่วนที่ 4 มีอักขระ 1 ตัว เป็นรหัสตรวจสอบความถูกต้อง

จากตัวอย่าง

974 แทน ประเทศไทย

472 แทนโรงพิมพ์นานมี

362 แทนการจำแนกหนังสือในโรงพิมพ์

และ $s \bmod 11$ เป็นตัวตรวจสอบ

โดยที่ s เป็น ผลบวกของผลคูณของตัวเลขโดดในรหัสกับตำแหน่ง

การเข้ารหัสและถอดรหัสแบบซีซาร์

การเข้ารหัสแบบซีซาร์เป็นวิธีการเข้ารหัสข้อความโดยเลื่อนตัวอักษรแต่ละตัวถัดไปอีก 3 ตำแหน่ง เช่น A เมื่อเข้ารหัสแล้วก็จะถูกเลื่อนไปเป็นอักษร D และตัวอักษร 3 ตัวสุดท้าย คือ X, Y และ Z จะเลื่อนไปเป็นตัวอักษร A, B และ C ตามลำดับ

วิธีการเข้ารหัสแบบซีซาร์จะกำหนด ตัวเลขแทนตัวอักษร โดยให้ A=0, B=1, ..., Z=25 เราจะเข้ารหัสโดยใช้ฟังก์ชัน $f(p) = (p+3) \bmod 26$

ตัวอย่าง 26 จงเข้ารหัสข้อความ “YESTERDAY” แบบซีซาร์

ตัวอย่าง 27 จงถอดรหัสข้อความ “WHQ” ที่ถูกส่งมาโดยใช้รหัวแบบซีซาร์

การเข้ารหัสและถอดรหัสแบบเชิงเส้น

$$f(p) = (ap + b) \bmod 26$$

โดย a, b เป็นจำนวนเต็ม และ f เป็นฟังก์ชันสมนัยหนึ่งต่อหนึ่ง

ตัวอย่าง 28 จงเข้ารหัสข้อความ “YESTERDAY” โดยใช้ฟังก์ชัน $f(p) = (7p + 3) \bmod 26$

ตัวอย่าง 29 จงถอดรหัสข้อความที่มีการเข้ารหัสโดยใช้ฟังก์ชัน $f(p) = (7p + 3) \bmod 26$